



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/666,847

09/18/2003

Perry Kiehtreiber

APLE.P0011

5767

48947

7590

12/16/2005

STATTLER, JOHANSEN, AND ADELI LLP
1875 CENTURY PARK EAST SUITE 1360
CENTURY CITY, CA 90067

EXAMINER

DARROW, JUSTIN T

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 12/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/666,847	Applicant(s) KIEHTREIBER ET AL.	
	Examiner Justin T. Darrow	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09/18/2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-20 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 3, 6, 8-11, 13-15, and 17-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Thomson Consumer Electronics, Inc. (Rohatgi et al.), European Patent Application Publication No. EP 0 752 786 A1.

As per claim 1, Rohatgi et al. discloses a method for sealing a computer program comprising:

dividing the computer program into a plurality of blocks (see page 7, lines 20-21; figure 7, step 41; determining modules from an application tagged with an index (i));

calculating a hash value for each of the blocks (see page 7, lines 32-33; figure 7, step 46; applying a hash function to the module);

creating a hash array with the hash values of the blocks (see page 8, line 2; figure 7, step 50; placing the have value $H(M(i))$ into the Directory Module);

digitally signing the hash array to create a digital signature (see page 8, lines 5-6; figure 7, step 51; the Directory Module is encrypted with the application provider's private key; see

Art Unit: 2132

page 8, lines 13-14; where the signing of the Directory Module is performed using the provider's private key); and

grouping the computer program with the hash array and the digital signature (see page 8, lines 7-10; figure 1, item 11; figure 7, step 53; attaching the encrypted hash value of the Directory Module, the Directory Module, and the program in the memory).

As per claim 3, Rohatgi et al. further points out:

distributing the computer program, the hash array, and the digital signature (see page 8, lines 9-12; transmitting the program with the Directory Module and the encrypted hash value).

As per claim 6, Rohatgi et al. also embodies:

storing the computer program, the hash array, and the digital signature together (see page 8, lines 7-10; figure 1, item 11; figure 7, step 53; attaching the encrypted hash value of the Directory Module, the Directory Module, and the program together for storage in the memory).

As per claims 8 and 18, Rohatgi et al. describes a method and computer-readable medium for authenticating a computer program comprising:

verifying the authenticity of a hash value array that accompanied the computer program by using a digital signature of the hash value array that accompanied the computer program (see page 11, lines 37-39; figure 10, steps 124 and 126; the Directory Module is applied to the hash function to produce a hash function compared to the decrypted Directory Module hash value (i.e. decrypted digital signature));

Art Unit: 2132

loading a block of the computer program (see page 11, lines 53-54; figure 10, step 136; accessing a module from memory);

calculating a calculated hash value for the block of the computer program (see page 11, lines 53-54; figure 10, step 138; applying the module to the hash function element and hashing it);

comparing the calculated hash value for the block of the computer program with an associated hash value for the block of the computer program from the hash value array (see page 11, lines 54-56; figure 10, step 140; the respective hash value is compared with the corresponding hash value transmitted in the Directory Module); and

generating an error if the calculated hash value for the block of the computer program does not match the associated hash value (see page 11, lines 55-56; figure 10, steps 150 and 152; if the hash values do not agree, errors are presumed generated and the module is discarded).

As per claims 9 and 19, Rohatgi et al. further elaborates:

calculating an array hash value for an array of hash values that accompanies the program; and (see page 11, lines 37-39; figure 10, step 124; the Directory Module is applied to the hash function to produce a hash function); and

comparing the array hash value with the digital signature of the hash value array using a public key (see page 11, lines 37-39; figure 10, step 126; the Directory Module is applied to the hash function to produce a hash function compared to the decrypted Directory Module hash value; see page 11, lines 31-34; decrypting the Directory Module hash value (i.e. digital signature) with the public key of the application provider).

Art Unit: 2132

As per claims 10 and 20, Rohatgi et al. then points out:

testing the digital signature with a public key and a public key encryption function (see page 11, lines 31-34; figure 11, step 1244; decrypting the Directory Module hash value (i.e. digital signature) with the application provider's public key).

As per claim 11, Rohatgi et al. also explains:

repeating the steps of loading, calculating, comparing, and generating as additional blocks of the computer program are needed for execution (see page 11, lines 53-59; figure 10, steps 136, 138, 140, 148; respective modules are accessed for checking for execution).

As per claims 13-15, Rohatgi et al. moreover discusses:

indicating an error message (see page 11, lines 35-36; figure 11, step 130; a warning is displayed).

As per claim 17, Rohatgi et al. then disclose:

swapping out the hash value array (see page 11, lines 34-35; figure 11, step 1241; the Directory Module is accessed from memory); and

re-verifying the authenticity of the hash value array after swapping the hash value array back in (see page 11, line 35; figure 11, step 1244; decrypting the encrypted Directory Module).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2, 4, and 5; and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson Consumer Electronics, Inc. (Rohatgi et al.), European Patent Application Publication No. EP 0 752 786 A1 as applied to claims 1 and 8, respectively, above, and further in view of Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C."

As per claims 2 and 12, Rohatgi et al. teaches the methods of claim 1 and 8. However, this reference does not explicitly describe a SHA hash value. Schneier discloses SHA (see section 18.7, pages 442; SHA designed for use with signatures). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the methods of Rohatgi et al. with the SHA hash value of Schneier because there are no known cryptographic attacks against SHA and it is more secure than 128-bit hash functions (see section 18.7, page 445).

As per claim 4, Rohatgi et al. then describes:

calculating an array hash value for the hash array (see page 8, lines 5-6; the hashed value H(M(i)) of the Directory Module); and

Art Unit: 2132

digitally signing the array hash value (see page 8, lines 5-6; the hashed value $H(M(i))$ of the Directory Module is encrypted with the application provider's private key; see page 8, lines 13-14; where the signing of the Directory Module is performed using the provider's private key).

As per claim 5, Rohatgi et al. next specifies:

creating the digital signature with a private key and a public key encryption function (see page 8, lines 5-6; figure 7, step 51; the Directory Module is encrypted with the application provider's private key; see page 8, lines 13-14; where the signing of the Directory Module is performed using the provider's private key).

6. Claims 7 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson Consumer Electronics, Inc. (Rohatgi et al.), European Patent Application Publication No. EP 0 752 786 A1 as applied to claims 1 and 8, respectively, above, and further in view of Bolosky et al., U.S. Patent Application Publication No. US 2002/0194484 A1.

Rohatgi et al. teaches the methods of claims 1 and 8. However, this reference does not explicitly describe an operating system. Bolosky et al. embodies an operating system (see ¶ [0061]; figure 3, item 358; an operating system as discrete blocks; see ¶ [0070]; figure 4, item 402; hashed and encrypted with the hash value used as an encryption key). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the methods of Rohatgi et al. with the operating system of Bolosky et al. to allow a user to quickly access a file, verify that it is indeed the requested file, all while insuring that the

Art Unit: 2132

files are stored and accessed in a secure way that prevents access by non-authorized users (see ¶ [0005]).

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to 571-273-8300 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an

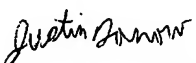
Art Unit: 2132

amendment after final rejection have printed not only **"OFFICIAL FAX"** but also **"AMENDMENT AFTER FINAL"**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

December 9, 2005


JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100